IF YOU ASSUME CONTRADICTION AXIOMS, YOU CAN DERIVE ANYTHING. IT'S CALLED THE PRINCIPLE OF EXPLOSION.

ANYTHING? LEMME TRY.

HEY, YOU'RE RIGHT! I STARTED WITH PA^P AND DERIVED YOUR MOM'S PHONE NUMBER!

THAT'S NOT HOW THAT WORKS.

WAIT, THIS IS HER NUMBER! HOW--
HI, I'M A FRIEND OF-- WHY, YES, I AM FREE TONIGHT!

MOM!
NO, BOX WINE SOUNDS LOVELY!
Proof Style for Number Theory

- We use predicate logic to make the proof claim very precise. However, please write the actual proofs in English, not logic!

- E.g. for all integers \( x \), if \( x \) is odd then \( x + 1 \) is even.

- Good: Let \( x \) be arbitrary. Suppose \( x \) is odd. Then \( x = 2k + 1 \) for some integer \( k \) ...

- Bad: Let \( x \) be arbitrary. Suppose \( \text{Odd}(x) \). Then \( \exists k \ (x = 2k + 1) \) ...
Number Theory: Motivation
Number Theory

- Branch of mathematics that deals with the properties and relationships of numbers
  - E.g. can we efficiently test if an integer is prime?
  - E.g. can we efficiently factor an integer?

- Many significant applications in computing
  - Cryptography & Security
  - Hashing

- Playground for practicing proof-writing
Modular Arithmetic

• Arithmetic over a finite domain

• In computing, almost all computations are over a finite domain
Modular Arithmetic

- public class Test {
-     final static int SEC_IN_YEAR = 365*24*60*60;
-     public static void main(String args[]) {
-         System.out.println("I will be alive for at least " + SEC_IN_YEAR * 100 + " seconds.");
-     }
- }

I will be alive for -1141367296 seconds.
Divisibility
Divisibility

- **Definition:**
  For integers $a, b$, we say $a \mid b$ ("$a$ divides $b$") iff there exists some integer $k$ such that $b = ka$.

- Informally: "$a$ fits into $b$" or "$a$ is a factor of $b$"

- **Examples:** $5 \mid 15$  
  $-3 \mid 9$  
  $5 \nmid 21$
Divisibility

- Which of these is true?

5 \mid 1 \quad 25 \mid 5 \quad 7 \mid 0 \quad -2 \mid 4

1 \mid 5 \quad 5 \mid 25 \quad 0 \mid 7 \quad 4 \mid -2
Division Theorem

- Division Theorem:
  For any integer $a$ and positive integer $d$, there exist unique integers $q, r$ with $0 \leq r < d$ such that $a = qd + r$. 
Division Theorem

- **Division Theorem:**
  
  For any integer $a$ and positive integer $d$, there exist unique integers $q, r$ with $0 \leq r < d$ such that $a = qd + r$.

- $q$ is referred to as the **quotient**

- $r$ is referred to as the **remainder**
Division Theorem

- Division Theorem:
  For any integer \(a\) and positive integer \(d\), there exist unique integers \(q, r\) with \(0 \leq r < d\) such that \(a = qd + r\).

- In Java, \(q\) is the result of the operation \(a/d\)
- In Java, \(r\) is the result of the operation \(a \% d\)

Warning
When dealing with negative numbers, Java’s \(\%\) may behave differently!
The mod (%) operator

- The % operator is often referred to as “mod”
- \( a \% d \) returns the remainder \( r \) when you divide \( a \) by \( d \)

\[
\begin{align*}
22 \% 5 &= 2 \\
25 \% 5 &= 0 \\
22 &= 4 \cdot 5 + 2 \\
25 &= 5 \cdot 5 + 0 \\
0 \% 5 &= 0 \\
-1 \% 4 &= 3 \\
0 &= 0 \cdot 5 + 0 \\
-1 &= -1 \cdot 4 + 3
\end{align*}
\]

Division Theorem
\( a = qd + r \) with \( 0 \leq r < d \)
Modular Arithmetic
Modular Arithmetic: Like a Clock

- Imagine you can only represent numbers 0, ..., 11. We call this "arithmetic mod 12".
- What’s 8 + 7? 3

Observation
The solution is \( a \mod 12 \).
Modular Arithmetic: Like a Clock

- Imagine you can only represent numbers 0, ..., 11. We call this “arithmetic mod 12”.
- What’s 3 − 5? 10

Observation
The solution is \( a \mod 12 \).
Modular Arithmetic: Like a Clock

- Imagine you can only represent numbers 0, ..., 11. We call this “arithmetic mod 12”.

What’s $3 \cdot 7$? 9

Observation
The solution is $a \% 12$. 
Modular Arithmetic: Generalizing

- We can extend modular arithmetic to clocks of any positive integer size.

E.g. $3 + 6$ in arithmetic mod 7 is 2
"Sameness"

- In modular arithmetic, many numbers have a notion of "sameness".
“Sameness”

- In modular arithmetic, many numbers have a notion of “sameness”.
  • To say “the same”, we don’t use the $=$ symbol.
    E.g. $13 = 1$ is wrong...
  • To say same in arithmetic mod $m$, we use the symbol $\equiv_m$
    - Pronounced “congruent mod $m$”
    - $13 \equiv_{12} 1$  $13 \equiv_{12} 25$  $2 \equiv_{12} 14$
    - $3 \equiv_{7} 10$  $0 \equiv_{7} 7$
**Congruence**

- We need a formal definition of $a \equiv_m b$.
  We can’t just say “$a$ and $b$ are on the same place in the $m$ clock 😊”

- **Definition:**
  For integers $a, b$ and positive integer $m$, we say $a \equiv_m b$ iff $m \mid (a - b)$.

- **Note:** $a \equiv_m b$ is equivalent to $a \% m = b \% m$.
  We will actually prove that the two notions are the same. But, the formal definition is much easier to use in proofs.
**Intuition**

- Here we have some groups of numbers that are congruent mod 10.

**Definition:** \( a \equiv_m b \) is defined as \( m \mid (a - b) \)

**Intuition:** Equivalently, \( a \equiv_m b \) means \( a \% m = b \% m \)
Properties of Congruence
Recall: Familiar Properties of $=$ in algebra

- If $a = b$, then $b = a$.
- If $a = b$ and $c = d$, then $a + c = b + d$.
- If $a = b$ and $c = d$, then $ac = bd$.
- If $a = b$ and $b = c$, then $a = c$.

- These are the facts that allow us to use algebra to solve problems. We will prove analogous facts for modular arithmetic.
Claim 1

Claim 1: For integers $a, b$ and positive integer $m$, if $a \equiv_m b$ then $b \equiv_m a$.

Proof

Let $a, b$ be arbitrary integers and let $m$ be an arbitrary positive integer.

Suppose that $a \equiv_m b$. Then by definition of congruence, $m \mid (a - b)$. Then by definition of divides, there exists some integer $k$ such that $a - b = mk$. Then multiplying both sides by $-1$, we have $b - a = -mk = m(-k)$. Since $k$ is an integer, $-k$ is an integer. So by definition of divides, $m \mid (b - a)$. Then by definition of congruence, $b \equiv_m a$. Since $a, b, m$ were arbitrary, the claim holds.
Note on Claim 1

- You’ll see $a \equiv_m b$ defined as $m \mid (a - b)$ or $m \mid (b - a)$ depending on where you look.
- Claim 1 proves these definitions are equivalent. From now on, you can use either definition in your proofs.
- In general, once we have proved claims in class, you can use those claims in your homework without proof.
Claim 2: For integers $a, b, c, d$ and positive integer $m$, if $a \equiv_m b$ and $c \equiv_m d$ then $a + c \equiv_m b + d$.

Intuition

$3 \equiv_{10} 13$ and $14 \equiv_{10} 24 \quad \Rightarrow \quad 17 \equiv_{10} 37$
Claim 2: For integers $a, b, c, d$ and positive integer $m$, if $a \equiv_m b$ and $c \equiv_m d$ then $a + c \equiv_m b + d$.

Proof

Let $a, b, c, d$ and $m > 0$ be arbitrary integers. Suppose that $a \equiv_m b$ and $c \equiv_m d$. Then by definition of congruence, $m \mid (a - b)$ and $m \mid (c - d)$. Then by definition of divides, there exists some integers $k, j$ such that $a - b = mk$ and $c - d = mj$. Then adding both expressions, we have:

$$a - b + c - d = mk + mj$$

$$(a + c) - (b + d) = m(k + j)$$

So by definition of divides, $m \mid (a + c) - (b + d)$. Then by definition of congruence, $a + c \equiv_m b + d$. Since $a, b, c, d, m$ were arbitrary, the claim holds.
Claim 3

Claim 3: For integers $a, b, c, d$ and positive integer $m$, if $a \equiv_m b$ and $c \equiv_m d$ then $ac \equiv_m bd$.

Intuition

$2 \equiv_{10} 12$ and $3 \equiv_{10} 13 \implies 6 \equiv_{10} 156$
Claim 3

Claim 3: For integers \(a, b, c, d\) and positive integer \(m\), if \(a \equiv_m b\) and \(c \equiv_m d\) then 
\[ac \equiv_m bd.\]

Proof (Attempt 1)

Let \(a, b, c, d\) and \(m > 0\) be arbitrary integers. Suppose that \(a \equiv_m b\) and \(c \equiv_m d\). Then by definition of congruence, \(m | (a - b)\) and \(m | (c - d)\). Then by definition of divides, there exists some integers \(k, j\) such that \(a - b = mk\) and \(c - d = mj\). Then multiplying both expressions, we have:

\[(a - b)(c - d) = mk \cdot mj\]

\[ac - bc - ad + bd = m^2 kj\]

Goal: \(ac - bd = mx\)
Claim 3: For integers $a, b, c, d$ and positive integer $m$, if $a \equiv_m b$ and $c \equiv_m d$ then $ac \equiv_m bd$.

Proof (Attempt 2):

Let $a, b, c, d$ and $m > 0$ be arbitrary integers. Suppose that $a \equiv_m b$ and $c \equiv_m d$. Then by definition of congruence, $m \mid (a - b)$ and $m \mid (c - d)$. Then by definition of divides, there exists some integers $k, j$ such that $a - b = mk$ and $c - d = mj$. Rearranging, we have $a = mk + b$ and $c = mj + d$. Multiplying both expressions, we have:

$$ac = (mk + b)(mj + d)$$

$$ac = m^2kj + mbj + mdk + bd$$

$$ac - bd = m^2kj + mbj + mdk$$

$$ac - bd = m(mkj + bj + dk)$$

Since $m, k, j, b, d$ are integers, $mkj + bj + dk$ is an integer. Thus by definition of divides, $m \mid ac - bd$. Then by definition of congruence, $ac \equiv_m bd$. Since $a, b, c, d, m$ were arbitrary, the claim holds.
Claim 4

- For integers $a, b, c$ and positive integer $m$, if $a \equiv_m b$ and $b \equiv_m c$ then $a \equiv_m c$.

Proof

Let $a, b, c$ and $m > 0$ be arbitrary integers. Suppose that $a \equiv_m b$ and $b \equiv_m c$. Then by definition of congruence, $m \mid (a - b)$ and $m \mid (b - c)$. Then by definition of divides, there exists some integers $k, j$ such that $a - b = mk$ and $b - c = mj$. Adding the expressions, we have:

$$(a - b) + (b - c) = mk + mj$$
$$a - c = m(k + j)$$

Since $k, j$ are integers, $k + j$ is an integer. Thus by definition of divides, $m \mid a - c$. Then by definition of congruence, $a \equiv_m c$. Since $a, b, c, m$ were arbitrary, the claim holds.

Definitions:

$a \mid b$ iff $\exists k \in \mathbb{Z} \ (b = ka)$

$a \equiv_m b$ iff $m \mid (a - b)$
Claim 5: For integers $a, b$ and $m > 0$, $a \equiv_m b$ if and only if $a \% m = b \% m$. 
For integers $a, b$ and $m > 0$, $a \equiv_m b$ if and only if $a \% m = b \% m$.

$\Rightarrow$ Let $a, b, m > 0$ be arbitrary integers, and suppose $a \equiv_m b$. Then $m \mid (a - b)$. So there exists some integer $k$ such that $a - b = km$. So $a = km + b$.

By the Division Theorem, $a = qm + (a \% m)$ for some integer $q$, where $0 \leq a \% m < m$. Thus:

$$km + b = qm + (a \% m)$$

$$b = qm - km + (a \% m)$$

$$b = (q - k)m + (a \% m)$$

By the Division Theorem again, we have that $b \% m = a \% m$.

Since $a, b, m$ were arbitrary, the claim holds.
For integers \(a, b\) and \(m > 0\), \(a \equiv_m b\) if and only if \(a \% m = b \% m\).

\[
\Leftrightarrow \text{Let } a, b, m > 0 \text{ be arbitrary integers, and suppose } a \% m = b \% m. \text{ By the Division Theorem, } a = mq + (a \% m) \text{ for some integer } q, \text{ and } b = ms + (b \% m) \text{ for some integer } s. \text{ Thus:}
\]

\[
a - b = (mq + (a \% m)) - (ms + (b \% m))
\]

\[
a - b = mq - ms + (a \% m) - (b \% m)
\]

\[
a - b = m(q - s)
\]

Since \(q, s\) are integers, \(q - s\) is an integer. So \(m \mid (a - b)\). So \(a \equiv_m b\).

Since \(a, b, m\) were arbitrary, the claim holds.
Summary: Properties of Mod

- Let \( a, b, c, d \) and \( m > 0 \) be integers.
  - If \( a \equiv_m b \), then \( b \equiv_m a \).
  - If \( a \equiv_m b \) and \( c \equiv_m d \), then \( a + c \equiv_m b + d \).
  - If \( a \equiv_m b \) and \( c \equiv_m d \), then \( ac \equiv_m bd \).
  - If \( a \equiv_m b \) and \( b \equiv_m c \), then \( a \equiv_m c \).
  - \( a \equiv_m b \) if and only if \( a \% m = b \% m \).